Department of Homeland Security Daily Open Source Infrastructure Report for 27 July 2005

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

For info click here
http://www.dhs.gov/

Please Help Improve the DHS Daily Infrastructure Report

We are striving to improve the DHS Daily Infrastructure Report for all of our readers. Please help us in this effort by filling out a short feedback form, which can be found by clicking on this link:

http://chrome.osis.gov/questionnaire

The form will only be available for two weeks, so please fill it out at your earliest convenience. Thank you in advance.

Daily Highlights

- The Christian Science Monitor reports federal agents say a new crisis is emerging along the southern border: non−Mexicans are crossing over the border in record numbers −− some from countries with terrorist ties −− and most are set free soon after being captured. (See item 8)
- The U.S. Food Safety and Inspection Service has issued revised emergency protocols for federal meat inspectors to follow after the declaration of a threat condition by the Department of Homeland Security. (See item 20)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *July 26, New York Times* — **In search of a new energy source, China looks to the wind.** China's skyrocketing energy needs have recently grabbed the world's attention through its bold efforts to take over foreign oil companies like the American oil independent Unocal. It has also made big investments in petroleum production in countries as far−flung as Sudan and Venezuela. However, at home, with petroleum growing scarce, coal choking the air of major cities and coal mining killing 6,009 people last year, the Chinese government is moving just as aggressively to develop alternative energy supplies. By 2020, starting from a minuscule base that it has established only recently, China expects to supply 10 percent of its needs from renewable energy sources, including wind, solar energy, small hydroelectric dams and biomass. "We have huge goals for wind power development," Wang Zhongying, director of China's Center for Renewable Energy Development. "By 2010, we plan to reach 4,000 megawatts, and by 2020 we expect to reach 20,000 megawatts, or 20 gigawatts." In February, the Chinese government passed a nationwide renewable energy law that formalizes many of those incentives and mandates clear targets for increased power generation from alternative energy sources. China's provinces will be required to buy electricity from alternative providers, even when the cost per kilowatt is substantially higher.
   Source: http://www.nytimes.com/2005/07/26/international/asia/26turbi ne.html?

2. *July 26, Government Accountability Office* — **GAO−05−611: Nuclear Security: DOE's Office of the Under Secretary for Energy, Science and Environment Needs to Take Prompt, Coordinated Action to Meet the New Design Basis Threat (Report).** A successful terrorist attack on a Department of Energy (DOE) site containing nuclear weapons material could have devastating effects for the site and nearby communities. DOE's Office of the Under Secretary for Energy, Science and Environment (ESE), which is responsible for DOE operations in areas such as energy research, manages five sites that contain weapons−grade nuclear material. A heavily armed paramilitary force equipped with such items as automatic weapons protects ESE sites. The Government Accountability Office (GAO) was asked to examine (1) the extent to which ESE protective forces are meeting DOE's existing readiness requirements and (2) the actions DOE and ESE will need to take to successfully defend against the terrorist threat identified in the October 2004 design basis threat (DBT) by DOE's implementation deadline of October 2008. To ensure that DOE and ESE protective forces can meet the terrorist threat contained in the 2004 DBT, GAO is making five recommendations to the Secretary of Energy to, among other things, address weaknesses with protective officers' equipment and coordinate ESE efforts to address the 2004 DBT. DOE concurred with the report, accepted GAO's recommendations and provided an update on actions it anticipated taking to address GAO's recommendations.
   Highlights: http://www.gao.gov/highlights/d05611high.pdf
   Source: http://www.gao.gov/new.items/d05611.pdf

3. *July 26, TheIndyChannel.com (IN)* — **Heat led to record electricity usage.** Indianapolis Power & Light Co. (IPL) said customers set a company record for electricity usage Monday, July 25, a day when afternoon temperatures in the city climbed into the 90s. Demand was at 3,118 megawatt hours at 3 and 4 p.m. Monday, breaking the previous record of 3,003−megawatt hours, set on July 22, 2002. IPL said its power generating system was

performing well, however, the company said it urges its customers to take measures to conserve energy.
Source: http://www.theindychannel.com/weather/4768021/detail.html

4. *July 23, The Japan Times* — **More Japanese nuclear plant data leaked via file−swapping program.** Data on nuclear power plant safety inspections in Japan have been posted on the Internet, apparently leaked through the Winny file−swapping program on a virus−infected personal computer of an employee at the Nuclear and Industrial Safety Agency, the agency said Friday, July 22. The leaked data include reports on inspections between 2000 and 2002, and information on the operational status of nuclear plants in Fukui, Niigata, Shizuoka and Kagoshima prefectures, according to the agency. An agency employee in charge of inspections of nuclear plants had taken the data home and worked on his personal computer when the data were leaked, it said. The personal computer is suspected to have been infected with a virus and the data are thought to have been leaked through Winny peer−to−peer file−sharing software, which was installed in the computer.
Source: http://www.japantimes.co.jp/cgi−bin/getarticle.pl5?nn2005072 3a5.htm

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *July 26, Richmond Times Dispatch (VA)* — **Chemical leak in Virginia.** A corrosive−acid leak caused the evacuation of a 12−block area in the City Point area of downtown Hopewell, VA, on Monday, July 25. Approximately 500 gallons of nitric acid spilled when a two−inch−thick hose broke during a transfer from a rail car to a truck. The leak was contained about 10 minutes after it started. The leak happened shortly before 3 p.m. (EDT) at Regional Enterprises, a small company with 52 employees that specializes in intermodal transport. The employee who was transferring the acid suffered second−degree burns on both forearms, his chest and leg, said Regional Enterprises' President Gary Farrar. Nine people were decontaminated at John Randolph Medical Center. Police went door−to−door in a residential area north of Appomattox Road telling people they needed to evacuate. Residents south of Appomattox Road were encouraged to stay inside and to keep their air conditioning off and windows shut, Hopewell Police Chief Rex Marks said. At approximately 9:20 p.m., it was determined that environmental conditions were safe enough for residents to return to their homes.
Source: http://www.timesdispatch.com/servlet/Satellite?pagename=RTD/MGArticle/RTD_BasicArticle&c=MGArticle&cid=1031784062516

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

6. *July 26, New York Times* — **Merchants could be the weak link in data protection.** While the banks and payment processors have been targets in the largest and highest−profile attacks of data thieves, security specialists say the payment system's most vulnerable points may be the estimated five million merchants where cards are accepted. Unlike banks and other financial institutions, merchants often lack technological expertise and management attention to keep their customers' information secure. The widespread use of wireless technology by businesses, as in homes, has left merchants' computer systems increasingly susceptible. Meanwhile, the credit card associations, like MasterCard and Visa, have been lax about enforcing their own security rules. The requirements for retailers to protect consumer data frequently fall through the cracks of government and industry regulations. "The breaches at processors and Internet gateways are very few and far between," said Bryan Sartin, a lead investigator for Cybertrust, a security services firm. "About 95 percent of what you are seeing right now are data breaches involving e−commerce merchants and retailers," said Sartin.
Source: http://www.nytimes.com/2005/07/26/business/26card.html

7. *July 26, AFX* — **EU proposes banks register details of all money transfers.** The European Commission (EU) is proposing that banks register the details of anybody transferring money in the EU in a further crackdown on terrorist funding. The commission said its proposal would help the relevant authorities in their action against terrorists and other criminals. Under the proposal, banks would be required to provide the authorities acting against terrorism or money laundering with the name, address and account number of anyone transferring money.
Source: http://www.iii.co.uk/news/?type=afxnews&articleid=5362333&format=reformatted&subject=economic&action=article

[Return to top]

Transportation and Border Security Sector

8. *July 26, Christian Science Monitor* — **Illegal entry by non−Mexicans rises.** After decades of attempting to dam the flow of Mexican immigrants crossing into the United States illegally, federal agents say a new crisis is emerging along the southern border. Non−Mexicans are spilling over the border in record numbers −− some from countries with terrorist ties −− and most are set free soon after being captured. The problem is that OTMs, or "Other Than Mexicans" as the Border Patrol classifies them, must be returned to their country of origin, they cannot be simply sent back across the southern border, as most Mexicans are. Under U.S. law, they must be detained pending a deportation hearing. Since immigration detention centers are packed, most OTMs are given a court summons and told to return in three months. At least 85 percent don't. In a hearing in the House Appropriations Subcommittee on Homeland Security earlier this month, Border Patrol Chief David Aguilar said his agency has apprehended 919,000 illegal immigrants so far this year −− 119,000 were OTMs. Most are from Brazil and Central America, but Aguilar reported that last year 644 came from "countries of concern."
Source: http://www.csmonitor.com/2005/0726/p01s01−usfp.html

9. *July 26, Associated Press* — **Westward Airways ceases operations.** Financially strapped Westward Airways of Scottsbluff, NE, has ceased operations, according to the airline's president. A message on Westward's reservations line said Monday, July 25, that all flights are temporarily suspended due to "operational issues" and said it would contact the caller once

operations resume. Westward Airways suddenly dropped its routes to Taos, Gallup, and Las Cruces in New Mexico last week. Westward had proposed returning to the New Mexico communities with reduced flights, but the suggestion was untenable to the cities, which argued Friday, July 22, that the airline had a responsibility under its contract to resume the original service. Westward began offering the routes last fall. Westward originally had cited non−payment of promised subsidies from the communities and a lack of passengers using those flights.
Source: http://www.usatoday.com/travel/news/2005−07−25−westward−air_x.htm

10. *July 26, Associated Press* — **Los Angeles to London flight diverted to Boston.** A flight from Los Angeles to London was diverted to Boston early Tuesday, July 26, because three Pakistani passengers were acting suspiciously, but nothing amiss was found and the three were released after questioning, authorities said. United Airlines Flight 934 landed in Boston shortly before 3 a.m. (EDT), Logan Airport spokesperson Phil Orlandella said. All three were later released and no charges were filed, said Gail Marcinkiewicz, a spokesperson for the FBI in Boston. Police searched the aircraft and found nothing suspicious, Orlandella said. State trooper Veronica Dalton said the three passengers had been "acting suspiciously and making the passengers nervous." The three passengers were not identified.
Source: http://www.nytimes.com/aponline/national/AP−Flight−Diverted. html?oref=login

11. *July 26, Department of Transportation* — **Regional railroad receives loan to improve service and safety in rural communities of Iowa and Illinois.** The Iowa Interstate Railroad (IIR) will receive a $32.7 million federal loan to help it improve service to rural areas that rely on trains to ship corn, soybeans, steel, chemicals and other products to market. The loan from the Federal Railroad Administration (FRA) will pay for track improvements needed to haul heavier freight cars and get products to key shipping points faster and safer. Besides helping companies such as Archer Daniels Midland, Maytag, and Midland Iron & Steel already located along its 571−mile line between Council Bluffs, Iowa, and Chicago, IL, the loan is expected to help the railroad lure new business and improve economic development in rural communities. The IIR connects to several railroads including the Union Pacific, Burlington Northern Santa FE, CSX, and the Iowa, Chicago & Eastern lines providing rail freight service to shippers across the Midwest and access to the national and global marketplace. The RRIF program is designed to help short line and regional railroads acquire, improve, or rehabilitate rail equipment and infrastructure or refinance previous debt incurred for that purpose.
Source: http://www.dot.gov/affairs/fra1905.htm

12. *July 26, Today* — **Canadian business coalition makes border recommendations.** One of the largest business coalitions in Canadian history has released its fourth report on the efficiency of the Canada−U.S. border since 9/11. The Coalition for Secure and Trade−Efficient Borders was formed by over 55 Canadian business associations and individual companies to help the federal government successfully deal with U.S. border and security issues. Steered by the Canadian Manufacturers and Exporters, the Canadian Chamber of Commerce, and the Canadian Federation of Independent Business, the group's goal is to recommend measures to facilitate the passage of low−risk goods across Canada's borders; to recommend ways to strengthen Canadian security, immigration, and border management; and to increase cooperation between Canada and the U.S. to prevent the entry of terrorists and illegal goods into each country. The Coalition supports the integration, cross accreditation and designation of Canadian and U.S.

Customs agencies and officers, and the establishment of shared facilities located on either side of the border. Like most other business groups that depend on U.S. trade, the coalition is urging governments to expedite infrastructure enhancements at border crossings −− specifically at Detroit−Windsor, which experts say is the international gateway most in need of a new crossing.
Web Links:
Canadian Manufacturers and Exporters: http://www.cme−mec.ca
Canadian Chamber of Commerce: http://www.chamber.ca
Canadian Federation of Independent Business: http://www.cfib.ca
Source: http://www.todaystrucking.com/displayarticle.cfm?ID=4221

13. *July 25, Transportation Security Administration* — **TSA expands explosives−detection capability to Newark Liberty International Airport.** The Transportation Security Administration (TSA) on Monday, July 25, announced that it has deployed an explosives detection trace portal to the passenger security checkpoint in Terminal A at New Jersey's Newark Liberty International Airport. This new trace portal machine exemplifies TSA's commitment to deploying state−of−the−art technology to our nation's airports in an ongoing effort to mitigate threats. Passengers identified as needing additional screening will pass through the trace portal. As passengers enter the trace portal, they will be asked to stand still for a few seconds while several "puffs" of air are released, dislodging microscopic particles from passengers that are then collected and analyzed for traces of explosives. A computerized voice indicates when a passenger may exit the portal. Screeners will take necessary and appropriate steps to resolve alarms. SA continues to increase its explosives detection capabilities and will announce the next round of airports to receive these machines by the end of the summer. TSA anticipates deploying 100 additional machines to the nation's largest airports by January 2006.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 014fff3

14. *June 23, Government Accountability Office* — **GAO−05−724: Air Traffic Control Operations: The Federal Aviation Administration Needs to Address Major Air Traffic Operating Cost Control Challenges (Report).** Dating back to 1997, numerous reports have highlighted the need for the Federal Aviation Administration (FAA) to better control the growth in its Air Traffic Services operating costs, which account for about $6.5 billion or over 80 percent of FAA's total annual operating costs. In February 2004, FAA established the Air Traffic Organization (ATO) to take over its entire Air Traffic operations and established cost control as a major focus. The Government Accountability Office (GAO) was asked to determine: (1) What is ATO's financial outlook for its operations? (2) To what extent is ATO taking actions to control its operating costs? (3) What are some options ATO should consider in developing its cost control strategy? GAO recommends that the FAA and ATO develop a cost control and savings strategy based on rigorous cost benefit analyses. Such analyses should determine the optimal structure for providing ATO services to different user groups while ensuring against adverse impacts on safety. Results of these analyses should be documented in a publicly available business plan that the ATO and its key stakeholders can use to build a sound business case for making the difficult but unavoidable structural changes needed to streamline its operations. FAA and ATO officials agreed to consider these recommendations and said they are currently preparing such analyses.
Highlights: http://www.gao.gov/highlights/d05724high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−724

[Return to top]

Postal and Shipping Sector

15. *July 25, Houston Chronicle (TX)* — **Officials investigating why $29,000 was hidden in package.** Federal authorities are working to unravel a mystery which they say involves two immigrants from India caught staying in the Houston, TX, area without legal documentation, possessing firearms and trying to use the United Parcel Service (UPS) to transport $29,000 in cash that they feigned was clothing to South Carolina. The investigation began after a UPS clerk in Mont Belvieu, TX, became suspicious of a customer Tuesday, July 19, who paid $80 to ship a package of "clothing" overnight. The customer, wearing an earpiece connected to a cell phone, appeared to be receiving instructions about the package from the device. This package was shipped, and then the same customer appeared the next day with a similar package that he said was clothing. Upon inspection of this package, three small boxes filled with stacks of $100 bills wrapped in carbon paper were found. A specially trained police dog was brought to the office to sniff the money. The dog "went crazy," indicating the cash might have been in contact with drugs or explosives, authorities said.
Source: http://www.chron.com/cs/CDA/rssstory.mpl/metropolitan/328194 0

[Return to top]

Agriculture Sector

16. *July 26, AgProfessional* — **Soybean rust reports from land grant universities available online.** The American Soybean Association (ASA) and Doane Agricultural Services Company have announced that updates from Asian soybean rust Extension specialists affiliated with the Land Grant Universities are now available on the Soybean Rust Advisory Program (SoyRAP) Website. Launched in May by ASA and Doane, the Website is an online resource containing advice from leading experts about combating soybean rust, rust's impact on the soybean markets, and news updates as they occur. Reports of soybean rust had been limited to a few isolated areas in Florida and Georgia prior to the arrival of Hurricane Dennis. Now the disease has been detected in Alabama and Mississippi and has spread to new counties in Florida and Georgia.
Website: http://www.SoyRAP.com
Source: http://www.agprofessional.com/show_story.php?id=34237

17. *July 26, Associated Press* — **Blackberry fungus enters U.S.** A deadly fungus used to control the spread of unwanted varieties of blackberries overseas has landed in the U.S., infecting the capital of America's blackberry industry. First spotted this spring on the southern Oregon Coast, the rust fungus has spread to seven counties, said officials with the Oregon Department of Agriculture. Initially, the species was only spotted on the Himalayan blackberry, a weed. Now it's also been reported in virtually all of the fields of the commercially grown evergreen blackberry, the number two blackberry crop in Oregon, accounting for roughly nine percent of the state's $30 million blackberry industry. Officials said it was too early to estimate the potential economic damage. The fungus has been used since at least the 1990s as a biocontrol

agent to tame the growth of wild blackberries in Australia, New Zealand, and Chile. Agriculture officials are meeting this week to begin discussing possible remedies. Once infected, the leaves of the blackberry bush become stained with a mosaic of purple spots. Underneath, the foliage is tainted with yellow pustules. While the disease has so far only been confirmed in Oregon, scientists and growers say it's already crossed into southwestern Washington, where samples taken from several fields are currently being tested for the fungus.
Source: http://www.wilmingtonstar.com/apps/pbcs.dll/article?AID=/20050726/APF/507260574&cachetime=5

18. *July 26, Associated Press* — **Eastern equine encephalitis reported in Virginia.** State agricultural officials Monday, July 25, confirmed Virginia's first two cases of Eastern equine encephalitis this year. Two horses from Chesapeake tested positive and four more are under evaluation, according to the state Department of Agriculture and Consumer Services. The department is advising horse owners to vaccinate their animals every six months to one year against the disease, which is generally transmitted by mosquitoes. There is no cure for the disease, but it generally can be prevented though vaccination. Chesapeake has experienced increased Eastern equine encephalitis activity this year, with 12 positive sentinel chickens and 40 positive mosquito pools, the department said.
Source: http://www.wavy.com/Global/story.asp?S=3639748&nav=23iicZ3E

19. *July 25, United Press International* — **New system can better reveal crop health.** Scientists have found firing rapid pulses of polarized light at corn and other crops provides a picture of plant health that's invisible to the naked eye. Using a portable light source and detector technology, the researchers said they can differentiate minute differences in leaf colors −− indicators of over− or under−fertilization −− crop−nutrient levels and perhaps even disease. The scientists hope their tractor−mountable N−Checker (for "nitrogen−checker") will help farmers determine in real time how much fertilizer to apply. The researchers −− from Containerless Research Inc. of Evanston, IL; the Chicago Botanic Garden and the University of Illinois −− said the N−Checker can take 1,000 measurements per second while moving at roughly five miles an hour.
Source: http://washingtontimes.com/upi/20050725−045347−3177r.htm

[Return to top]

Food Sector

20. *July 20, Food Safety and Inspection Service* — **Protocols issued for inspectors in U.S. food plants.** The U.S. Food Safety and Inspection Service has issued revised protocols for plant inspectors. Following declaration of a threat condition by the Department of Homeland Security, U.S. federal meat inspectors will notify plant management of implementation of new Food Defense Verification Procedures, which will take immediate priority over other assigned inspection tasks. With a yellow alert not specific to the food and agriculture sector, the inspector in charge (IIC) will evaluate one of the following food−defense areas, chosen randomly: outside premises, control/use of hazardous chemicals, live animal health (slaughter plants only), equipment calibration, loading dock and shipping areas, incoming raw materials, maintenance activities, storage areas, water systems, production/processing, or employee behavior. With an orange alert specific to the food and agriculture sector, the IIC will evaluate

three of the food−defense areas listed above, randomly chosen. Additional actions may be prescribed by the FSIS district office. These inspection activities will be unscheduled procedures within the establishing tour of duty and after all food safety procedures are performed. With a red alert specific to the food and agriculture sector, the IIC will evaluate all of the food−defense areas listed above in addition to taking any other action prescribed by the district office.
Source: http://www.fsis.usda.gov/OPPDE/rdad/FSISDirectives/5420.1_Re v2.pdf

[Return to top]

Water Sector

21. *July 25, Associated Press* — **Los Angeles water agency ordered to restore Owens River.** An Inyo County judge ordered the city of Los Angeles' water department Monday, July 25, to either act on repeated court orders to restore the Lower Owens River or stop pumping water from it. Superior Court Judge Lee E. Cooper ordered the Department of Water and Power to stop pumping water from one of its aqueducts but stayed the decision pending the city's compliance with orders to reduce its groundwater pumping by a third and begin recharging Owens Valley groundwater, the attorney general's office said in a statement. The city will also be required to pay a $5,000 per day fine beginning October 5 and must begin sending flows to the Lower Owens River by January 2007 as part of a project to help restore the area. "Today's court decision makes it perfectly clear that the law must be followed," California Attorney General Bill Lockyer said in the statement. The decision is the latest chapter in more than three decades of litigation. The events surrounding the Owens River, about 250 miles north of Los Angeles, go back to 1913, when an aqueduct was built to bring water from Inyo County to Los Angeles' fast−growing San Fernando Valley, turning the once fertile Owens Valley into a dust bowl.
Source: http://www.mercurynews.com/mld/mercurynews/news/local/states/california/northern_california/12221736.htm

[Return to top]

Public Health Sector

22. *July 26, BBC News* — **Flu mutates faster than thought.** Flu viruses can swap many genes rapidly to make new resistant strains, researchers have found. Scientists previously believed that gene swapping progressed gradually from season to season. The National Institutes of Health team found instead, influenza A exchanged several genes at once, causing sudden and major changes to the virus. The findings suggest strains could vary widely each season, making it potentially harder to treat. Each year, experts must predict which strains will be most common and design new vaccines to fight them. David Lipman and colleagues looked at strains of influenza A that had circulated between 1999 and 2004 in New York. These strains had given rise to the so−called Fujian strain H3N2 that caused a troublesome outbreak in the 2003−2004 flu season because the vaccine made that winter was a poor match for the virus. Lipman's team found wide variations in the 156 strains that they analyzed. Some of the strains had at least four gene swaps that had occurred in a short time period. This suggests that

scientists need to study circulating flu viruses more carefully because important mutations can occur suddenly and without warning, they said.
Research: http://biology.plosjournals.org/perlserv/?request=get−document&doi=10.1371/journal.pbio.0030300
Source: http://news.bbc.co.uk/1/hi/health/4717183.stm

23. *July 26, McKinney Courier Gazette (TX)* — **County to test new antibiotic dispensing system.** On August 9, Collin, TX, Health Care Services will test its antibiotic dispensing capabilities by staging a bioterrorism event. Collin County, along with Dallas, Tarrant, Denton, Hill, and Van Zandt counties, will practice sharing a shipment of antibiotics from the Strategic National Stockpile and distributing them among their cities in an exercise sponsored by the Texas Department of State Health and the U.S. Centers for Disease Control and Prevention. Collin County recruited volunteers in the medical field to help with the exercise. Many of the doctors and nurses who volunteered would be called upon by the county to assist in case of an actual emergency. The event is one of the largest regional distribution exercises in the country because of the expected participation among the seven counties.
Source: http://www.courier−gazette.com/articles/2005/07/25/news/news 01.txt

24. *July 26, Chicago Sun−Times (IL)* — **Mosquitoes with West Nile virus are widespread, experts warn.** Even though mosquitoes don't seem to be biting much, health officials are warning this could be an especially bad year for the mosquito−borne West Nile virus. A statewide sampling system is finding that the virus−carrying mosquitoes are as widespread now as they were at this point in 2002, when Illinois led the nation in West Nile infections. The Illinois Department of Public Health said Monday, July 25, with the addition of a positive bird sample in Kankakee County, 22 counties have been identified so far this year with West Nile virus activity. Other disease−carrying birds or positive mosquito samples have been identified in counties including Cook, DeKalb, DuPage, Peoria, Kane, McHenry, Lake, and Will. In Illinois in 2002, there were 884 West Nile cases and 67 deaths. Most cases were reported in late summer and fall. The number of cases was down sharply in 2003 and 2004, when the weather didn't favor Culex mosquitoes. It's impossible to predict how many cases will occur this year.
Source: http://www.suntimes.com/output/news/cst−nws−westnile26.html

25. *July 26, Associated Press* — **Bird droppings linked to Indonesia deaths.** Three family members who died of bird flu earlier this month were infected by chicken droppings that contained the deadly H5N1 strain of the virus, Indonesia's agriculture ministry said Tuesday, July 26. The three, a 38−year−old government official and his two young daughters, are the only people known to have died of the disease in Indonesia. Authorities earlier said they had no known contact with poultry but since found chicken feces in their backyard that "positively contained the bird flu virus," said Hari Priyono, an agriculture ministry spokesperson.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/07/26/AR2005072600212.html

26. *July 25, University of Georgia* — **Understanding biases in epidemic models important when making public health predictions.** Mathematical models have become invaluable decision−making tools for public health officials. Models can be useful in two ways: they can reveal the underlying characteristics of an infection and they can allow the comparison of alternative control measures. Often, however, such models make implicit assumptions that may

systematically bias their predictions. Researchers showed that commonly used disease models may risk making overly optimistic predictions about the levels of public health interventions needed to bring a disease under control. They found that many off−the−shelf models used in infection management do not realistically account for the length of time that people harbor infections. The simplest models entirely ignore the latent period of a disease: the period of time when an individual is infected but not yet infectious. Other models often assume that the rate of progression from latent to infectious, and infectious to recovered, is constant, irrespective of the time already spent in that status. “Models which do not incorporate the latent period or assume unrealistic distributions of the latent and infectious period,” said the researchers, “always resulted in underestimating the transmission potential of an infection when fitted to initial outbreak data.”
Research: http://medicine.plosjournals.org/perlserv/?request=get−document&doi=10.1371/journal.pmed.0020174
Source: http://tt.uga.edu/tt/http://www.uga.edu/news/artman/publish/050725wearingrohani.shtml

[Return to top]

Government Sector

27. *July 25, GovExec* — **New DHS policy office will tackle border security.** Department of Homeland Security Secretary Michael Chertoff said Monday, July 25, that the department's newly proposed policy office would develop a comprehensive strategy for improving the nation's border security and addressing illegal immigration. Chertoff proposed creating a departmentwide policy directorate, headed by an undersecretary, as part of several organizational changes announced two weeks ago. Since then, Chertoff has said the department is mapping out changes across the nation's border and immigration system, and plans to hire a program manager to execute more reforms in the coming months. "Obviously we know there's a huge issue with the border," Chertoff told government officials Monday during a keynote speech at the Excellence in Government conference in Washington, DC.
Remarks by Secretary Chertoff at the Excellence in Government Conference: http://www.dhs.gov/dhspublic/display?content=4683
Source: http://www.govexec.com/story_page.cfm?articleid=31839&sid=28

[Return to top]

Emergency Services Sector

28. *July 26, Federal Computer Week* — **Tampa law agencies form network.** Law enforcement agencies in the Tampa Bay region in Florida are forming a regional information−sharing network to aid their fight against organized crime, gangs, drug trafficking activities and terrorism. Using technology called CopLink, investigators will be able to search through vast quantities of information on individuals, organizations, locations, documents, vehicles, weapons and property stored in multiple databases across the region. CopLink, has been deployed in more than 130 jurisdictions nationwide. The Tampa Bay Security Network will be launched in three phases and will ultimately be integrated with other regional networks to form

a statewide information−sharing network. By July 2006, all 58 law enforcement agencies across the nine counties that comprise the Tampa Bay Regional Domestic Security Task Force will be part of the network. Eventually, it will be linked to the six other regional law enforcement information−sharing projects supported by the Federal Department of Law Enforcement.
Source: http://www.fcw.com/article89687−07−26−05−Web

29. *July 26, Associated Press* — **New York police study London bombing.** With New Yorkers still on edge after the terrorist attacks in London, the New York Police Department (NYPD) recently dispatched an explosives expert to Britain to study the suicide bombings. An NYPD detective with explosives training recently returned to New York "with a detailed analysis of the bomb−making techniques used in London," said Michael Sheehan, NYPD's deputy commissioner of counterterrorism. The police department also has contacted chemical suppliers and other potential commercial sources for suspected bomb components in the New York city area and asked them to contact investigators if they notice anything suspicious, officials said Monday, July 25. Sheehan said the department has conducted hundreds of security assessments of businesses around the city, advising them to use more video surveillance, better lighting and more guards.
Source: http://www.cnn.com/2005/US/07/26/ny.security.ap/index.html

30. *July 26, The Paris News (TX)* — **Terror drill in Texas tests emergency response.** About 50 people gathered Tuesday, July 26, in the Emergency Operations Center in Paris, TX, to begin a 2−1/2 day exercise to identify local officials' readiness to handle a terrorist attack. People with scanners heard reports of an "explosion" at the city water treatment plant about 9:45 a.m., followed shortly after 10 a.m. by reports of "chemical agents" discovered in the water at the plant. John Garnecki, who is with the National Emergency Response and Rescue Training Center, reminded the crowd of local officials from every branch of emergency response that terrorist attacks generally involve multiple events, such as what happened on September 11, 2001, in New York City, and recently in London. "Keep in mind that you as a responder can potentially be a victim. You can be a target and your facilities can be a target," Garnecki said.
Source: http://web.theparisnews.com/story.lasso?wcd=21747

31. *July 25, Federal Computer Week* — **Feds more prepared for emergencies.** Results from the Office of Personnel Management's annual survey of agencies' emergency planning efforts reveal higher levels of preparedness compared with a year ago. Responses from 85 organizations, including all 15 Cabinet−level agencies, show what OPM officials say are significant improvements in business continuity planning. For example, more than 95 percent of agencies surveyed conducted evacuation drills in the past year, 95 percent tested their fire safety and public address systems, 90 percent distributed emergency guides to employees, and more than 75 percent met with employees to discuss risks and contingency plans. To help safeguard federal workers with disabilities, the Labor Department's Office of Disability Employment Policy created a Web page devoted to emergency preparedness.
OPM Survey: http://www.opm.gov/emergency/EPSurvey2005/
Department of Labor Website: http://www.dol.gov/odep/programs/emergency.htm
Source: http://www.fcw.com/article89679−07−25−05−Web

[Return to top]

Information Technology and Telecommunications Sector

32. *July 25, FrSIRT* — **Netscape Browser security update fixes multiple vulnerabilities.** Two vulnerabilities were identified in Netscape Browser, which could be exploited by malicious Websites to execute arbitrary commands. The first issue is due to an input validation error in the processing of java script URLs opened by media players, which could be exploited by attackers to execute arbitrary code. The second vulnerability is due to an improper cloning of base objects, which could allow web content scripts to walk up the prototype chain to get to a privileged object and execute arbitrary code. Netscape Browser version 8.0.2 and prior are affected.
Users should upgrade to Netscape Browser version 8.0.3.1:
http://browser.netscape.com/ns8/download/default.jsp
Source: http://www.frsirt.com/english/advisories/2005/1214

33. *July 25, remote.com* — **ClamAV Library RemØte heap overflows security advisory.** ClamAV Antivirus Library is vulnerable to buffer overflows allowing attackers complete control of the system. These vulnerabilities can be exploited remotely without user interaction or authentication through common protocols such as SMTP, SMB, HTTP, FTP, etc. Specifically, ClamAV is responsible for parsing multiple file formats. At least four of its file format processors contain remote security bugs. Specifically, during the processing of TNEF, CHM, & FSG formats an attacker is able to trigger several integer overflows that allow attackers to overwrite heap data to obtain complete control of the system. These vulnerabilities can be reached by default and triggered without user interaction by sending an e−mail containing crafted data. Successful exploitation of ClamAV protected systems allows attackers unauthorized control of data and related privileges. ClamAV 0.86.1 (current) and prior are affected.
Users should upgrade to Clam Antivirus (ClamAV) version 0.86.2 :
http://sourceforge.net/project/showfiles.php?group_id=86638& release_id=344514
Source: http://www.rem0te.com/public/images/clamav.pdf

34. *July 25, Security Focus* — **PHPFirstpost Block.PHP remote file include vulnerability.** Phpfirstpost is susceptible to a remote PHP file include vulnerability. This issue is due to a failure in the application to properly sanitize user−supplied input. An attacker may exploit this issue to execute arbitrary PHP code on an affected computer with the privileges of the Web server process. This may facilitate unauthorized access. Currently Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/14371/info

35. *July 25, Security Focus* — **FTPLocate remote command execution vulnerability.** FtpLocate is prone to a remote arbitrary command execution vulnerability. This issue presents itself due to insufficient sanitization of user−supplied data. An attacker can supply arbitrary commands and have them executed in the context of the server. This issue may facilitate unauthorized remote access to the computer running the hosting Web server. Currently Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/14367/discuss

36. *July 25, FrSIRT* — **GoodTech SMTP Server remote buffer overflow vulnerability.** A vulnerability was identified in GoodTech SMTP Server, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to a buffer overflow error in smtpd when processing a specially crafted "RCPT TO" command, which could be exploited by attackers to compromise a vulnerable system. GoodTech SMTP Server for Windows NT/2000/XP/2003 version 5.16 and prior are affected.
Users should upgrade to GoodTech SMTP Server version 5.17:
http://www.goodtechsys.com/smtpdnt2000.asp
Source: http://www.frsirt.com/english/advisories/2005/1199

37. *July 25, TechWeb* — **Hackers spreading spyware from free personal Websites.** Attackers are using free personal Web hosting sites provided by nationally− and internationally−known ISPs to store their malicious code, and to infect users with worms, viruses, and spyware, a security firm said Monday, July 25. Websense, a San Diego, California−based Web security and content filtering vendor, has detected a big jump in the use of personal hosting sites, said Dan Hubbard, the company's senior director of security and technology research. "Attackers don't have to go to the trouble to find a compromised machine, search for one with a vulnerability they can exploit to turn into a zombie," said Hubbard. "Plus, they're reliable. Since they're offered up by national and international Internet service providers, they're built on a lot of infrastructure. Third, they often offer quite a bit of storage space, in some cases up to 500MB." The problem is that too few free hosting services offer even the most basic security tools, Hubbard said. None of the services found hosting malicious sites use a graphics−based question to make sure that a human, not a bot, registers for the service, he said.
Source: http://www.techweb.com/wire/security/166402258

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT has received reports of root−level attacks being distributed by SDBot variants, possibly involving Port 10102 activity, increased scanning of port 1433, probably related to the new MySQL vulnerabilities (See below), and scanning of Port 22 (SSH), probably related to recently reported SSH vulnerabilities and Hacker use of SSH to provide themselves with secure, hidden access to compromised systems. Please watch your flows and be alert for the appearance of new applications/daemons connecting to the Internet.

A remotely triggerable access violation error has been reported in Veritas NetBackup version 5.1. The issue occurs in the NDMP service (TCP port 10000) when a 'config' message request is handled that contains a 'TIME_STAMP' value that is out of range. The information that was posted discussed only a Denial of Service attack for this issue, however the full scope and severity of this vulnerability is not currently known for certain.

Additionally, an exploit module for the Metasploit Framework, which targets the Veritas Backup Exec Remote Agent for Windows Servers Authentication Buffer Overflow Vulnerability (BID 14022), which is accessible over TCP port 10000, was made available on June 24, 2005, and shortly after, widespread exploitation was recorded.

As a precaution, Administrators are advised to filter TCP port 10000 at the network perimeter until further research in regards to this issue is completed.

Current Port Attacks

Top 10 Target Ports	6346 (gnutella−svc), 1026 (−−−), 6881 (bittorrent), 445 (microsoft−ds), 1433 (ms−sql−s), 27015 (halflife), 135 (epmap), 139 (netbios−ssn), 80 (www), 4672 (eMule) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

38. *July 25, The Stamford Advocate (CT)* — **Connecticut school to get security cameras.** A Connecticut school district plans to install security cameras in the hallways and stairwells of Stamford High School, in Stamford, CT, which administrators said will make it easier to ensure the safety of 2,000 students. Cameras have become ubiquitous in public schools though some only monitor the exterior. In a 2002 survey by the U.S. Department of Education, 41 percent of administrators said their schools use cameras. The cameras are not meant to be invasive and will not be installed within classrooms. The security proposal calls for 360−degree cameras to monitor the teacher and student parking lots and fixed cameras in corridors and elevators, stairwells and school entrances. The cameras could zoom in to identify faces; this footage would be archived and could be reviewed in the school and remotely.
Source: http://www.stamfordadvocate.com/news/local/scn−sa−schoolsecurity5jul25,0,4847792.story?coll=stam−news−local−headlines

39. *July 20, WAVE 3 News (KY)* — **School bus drivers taking terrorism training in Kentucky county.** Thousands of children in Kentucky will be under increased security this year on the way to and from school. Jefferson County, KY, school bus drivers are among those now required to take terrorism training classes. David Breitenstein, one of the trainers of bus security, says they'll be checking their vehicles each day for signs that "somebody's changed something, somebody's cut a brake hose, anything out of the ordinary." Once on the road, drivers have been instructed on how to identify and report suspicious activity. Also new this year, security cameras and motion detectors have been installed at all the bus compounds around the county, at a cost of $100,000. The goal is to make sure that no buses inside the compounds are tampered with overnight. Other school systems in Kentucky and Indiana are also requiring terrorism training for bus drivers this year.

Source: http://www.wave3.com/global/story.asp?s=3615882

[Return to top]

General Sector

40. *July 26, ClickOnDetroit* — **Pipe bomb discovered along I−94.** A pipe bomb discovered along the side of Michigan's Interstate 94 on Monday night, July 25, has sparked an investigation. A passerby discovered the five−inch−long pipe bomb on a guard rail along the I−94 service drive at Haggerty Road, Detroit's Local 4 News reported. The bomb squad used a robot to retrieve the device, the station reported. The squad determined the pipe bomb was real.
Source: http://www.clickondetroit.com/news/4769248/detail.html?subid=22100415&qs=1;bp=t

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer